Sonera SmartTrust Ltd, P.O. Box 425, FIN-00051 SONERA, Elimäenkatu 17-19, Helsinki, Finland
T +358 (0) 2040 63031 F +358 (0) 2040 62730 E info@smarttrust.com www.smarttrust.com

WHITE PAPER
Basic Elements of a PKI

By Sten Lannerstrom

Last updated: 8 Dec 2000

Sonera SmartTrust Ltd, P.O. Box 425, FIN-00051 SONERA, Elimäenkatu 17-19, Helsinki, Finland
T +358 (0) 2040 63031 F +358 (0) 2040 62730 E info@smarttrust.com www.smarttrust.com

Table of Contents

Sonera SmartTrust Ltd, P.O. Box 425, FIN-00051 SONERA, Elimäenkatu 17-19, Helsinki, Finland
T +358 (0) 2040 63031 F +358 (0) 2040 62730 E info@smarttrust.com www.smarttrust.com

Abstract

Asymmetric encryption, using private keys in combination with certificates, allows users to identify themselves over an electronic network, to communicate privately, and to sign electronic documents. These functions form the basis for e-commerce, and a system that exploits this technology is known as a Public Key Infrastructure (PKI). .

Internet Business demands a PKI

Asymmetric encryption, using private keys together with certificates, allows users to identify themselves over an electronic network, to communicate privately and to sign electronic documents. The administration of - and ability to use - certificates and public and private keys, provides the enabling structure for e-transactions based on this concept. This underlying structure forms a Public Key Infrastructure (PKI).

It is almost impossible to establish a working Public Key Infrastructure without a common carrier of data that is easily accessible by the general public. Or, to put it another way, without a commonly accepted method of connecting computers there is simply no need for a PKI. This is probably why large scale PKI has not made greater strides already, despite the fact that the technology has been around for more than two decades. However, the increasing use of home based computers, the expansion of the Internet, and market exposure resulting from this “new” information transport system are now providing a catalyst for innovative ways of doing business.

The virtual marketplace is much less expensive to invent, and faster to develop, than its physical counterpart. Formerly accepted laws of the market are, if not set aside completely, subject to disruption. It is, perhaps, inappropriate to compare the virtual marketplace with the physical one, but nevertheless they both offer companies space to do business. Cyberspace has made it possible for newcomers in various business segments to compete with well-established larger competitors.

The new market has put great pressure on organizations that are successful, comfortable and have a stable business in the traditional marketplace, to adapt and find viable ways of doing business in the virtual arena. Without going into further analysis of the potential winners and losers in

Cyberspace, there's a common factor essential to success in the virtual marketplace - the act of non-repudiation, binding customers and businesses to contracts. Traditional methods of signing agreement orders, etc. must be reproduced electronically. PKI provides the means to do this.

Without the ability to create legally binding contracts between remote parties electronic commerce will be unable to reach its full potential.

Security Services

The general purpose of a PKI is to enable security across networks and to provide the means to remotely identify a user and to establish methods, which imitate - and possibly improve - the written signature.

There are four security services that must be in place before a viable e-business can evolve. These services are 1) authentication 2) confidentiality 3) integrity 4) non-repudiation.

Authentication

Verifying that a user actually is who s/he claims to be. In the physical world, this is commonly accomplished by use of a passport, driving license or ID card. (in some countries a credit card is acceptable for this purpose, although without a photograph credit cards cannot provide true authentication). From an e-commerce perspective it must be possible to verify the identity of a user remotely.

Confidentiality

Confidentiality means ensuring that no one other than the expected parties is able to see an ongoing dialogue. In the physical world appropriate levels of confidentiality are assured by means such as voice control, choice of location, time, etc. In the virtual world it is more difficult to know who might be listening. Thus, in the virtual world, services which offer an assurance of confidentiality take on a more crucial role.

Integrity

This means ensuring that a message cannot be altered in any way during transmission. There has always been a demand for integrity when two or more remote parties need to rely on a given quantity of information. In the virtual world the traditional seal has been replaced by a digital signature.

Non-repudiation

Non-repudiation is the act of assuring the origin and/or issuance of a transaction or action. A physical agreement is likely to be produced on a paper document of some sort; most likely the date will be written on it prior to signing the document, and the procedure will be monitored by the other party, which will then also sign the document.

This procedure is then repeated, setting up two identical agreements, or one party will get a copy, allowing it to claim verification in case of a dispute. In the virtual world it is equally necessary to create statements that, firstly, state an origin and secondly, can be verified at a later stage.

PKI setup and the major players

Remember what PKI stands for, and especially the last word, infrastructure. Once the PKI is established it should serve all kinds of e-commerce, or in other words, any electronic business transaction conducted over an electronic network, either public or enterprise-wide. Once the PKI is in place the end user will probably not give much thought to the new application provider. The security routines involved in determining trust, and the procedures involved in storing a trusted server CA certificate, will become as natural as determining trust before taking the decision to buy something in a physical shop. The PKI itself is the ground upon which e-business applications are built, and through which e-commerce transactions flow.

There are four key elements within a PKI, they are:

1. The Certification Authority (CA)

- Issues and revokes certificate.
- Delivers the certificate to the end-user.
- Distributes the certificates and certification revocation lists to a Certificate repository.

2. The Certificate Repository

- Enables both end-users and end-entities to search for certificates and CRLs.

3. The End-users

- Requests certificates from a CA.
- Receives the certificate from the CA on a PKI card or floppy disk.
- Uses the certified keys and certificates in PKI enabled application services, thus enabling support for strong authentication, encryption and non-repudiation.
- May search the certificate repository for certificates and status information.

4. The Service Provider

- (Requests and receives its certificate from the CA).
- Provides application services based on PKI, thus enabling support for strong authentication, encryption and non-repudiation.

The Certification Authority

The CA is the authority that issues and revokes certificates. Providing assurance that the certified information is correct, and that the key used for signing certificates and CRLs is not compromised, are among the responsibilities of the Certification Authority.

Certification Authorities are bound by a number of other regulations too, but these are probably the most important ones.

A PKI smart card-based medium for private key storage and operation requires secure routines, including secure transportation from the manufacturer or supplier to the CA, as well as from the CA to the end-user. A further requirement of such a medium is that the PKI smart cards used are sourced from a trusted manufacturer. As the issuing authority, the CA must provide a reliable operation of the certificate management system and assure delivery of CRLs at scheduled occasions. The CA organisation must provide for well-developed audit capabilities without increasing the risk of exposure.

Examples of CA's would typically be (but are not limited to):

- Governmental organisations such as public post or telephony for public purposes
- Large corporations for internal purposes
- Telecom operators for secure m-commerce
- Banks for customers or internal purposes
- Banking organisations for internal purposes
- Trusted Third Party organizations for public purposes

The Certificate Repository

It is the function of the repository to store certificate and CRL information (CRLs are lists of revoked certificates; the issuing CA digitally signs each list). As an end-user and, possibly more importantly, as an end-entity, access is required to the repository where the relevant CA has placed certificates and CRL's. This repository is the source of the latest status information for a given certificate. It is also the place to undertake a certificate search in cases where e-mail encryption to a specific user is desired, and there is therefore a requirement for the user's public key. Within an organization, this information would probably be stored in the internal address book.

To serve as many end-users and end-entities as possible the repository must provide for good capacity throughput and, not least, provide a commonly accepted interface for the requester. A common interface, and well-used protocol, is LDAP (Lightweight Directory Access Protocol); while X.500 provides a common repository (database) structure.

It is probable that the repository will cater for more than simply certificate information. The important factor about certificate information is that it is signed by the CA, making it easy for the requestor to verify data integrity (given that the issuing CA is trusted).

The end-user

The end-user is typically someone using PKI enabled services over the Internet from a personal computer. This service could be a relatively new one, such as e-banking, or a well-established one, such as electronic mail. Outgoing mail may be encrypted by utilising the expected receiver's public key.

Given the contents of a typically S/MIME structured message, the receiver can verify the signature of the sender. The same applies to other PKI enabled services, such as electronic banking from the home or e-shopping, although the structure of the signed message may be a different one, for instance PKCS#7.

The structure of the actual message is not the relevant issue; the important thing is that it is possible to create a legally binding contract between the end-user and the service provider (end-entity) and vice versa.

The Service Provider

The service provider is the typical application service point, be it a banking application, e-mail server or any other PKI enabled application. The server is likely to be connected to a back-end system, providing the actual application database etc. Although not explicitly shown in the figure, the end-entity would most probably be equipped with a firewall to protect it from unwanted attempts to access the server. Once the end-user and end-entity have authenticated themselves the confidentiality security service is initiated. All data transport between the end-user and end-entity takes place in an encrypted format from that point on, thus reassuring both parties that data transferal is confidential during transmission.

Central processes in a PKI

Issuing certificates

The CA issues certificates to end-users and end-entities according to defined CA-policies. By issuing an X.509 certificate the CA binds the certified public key to a specific end-user or end-entity, thus logically also binding the private key. It is vital that information within the certificate is correct, since the CA has signed this information and an independent third party may verify that the CA issued the certificate.

The end-user or end-entity will use the certificate and the keys in combination with the certificate for authentication, and possibly signature operations. It is usual to provide certificates with different extensions that define the purpose of the certificate, such as authentication, confidentiality and non-repudiation.

A certificate is typically issued for a limited time period. This period will depend on the purpose of the certificate. A certificate which identifies a user as an individual may last for several years but certificates within a single sign-on system may last only for a limited period.

Revoking certificates

A certificate may be revoked whenever the private key of an end-user or end-entity is lost or if there is a suspicion that the private key has become exposed. This process normally takes place after the party owning the private key directs the CA to revoke the certificate. Revoked certificates are placed on a special list signed by the CA. This list is called a Certification Revocation List (CRL). The CRL will be distributed to a predefined and well-known place on a regular basis.

Once a certificate is revoked there is no longer a bond between the former owner and the keypair. It will still be possible to determine the previous owner, but the binding period ends. Thus it is still possible to verify a signature that was made before the certificate was revoked, but new authentication services or signatures should not be accepted.

The binding of a keypair with a given owner also expires when the certificate expires. This is a different issue and has nothing to do with revocation, although the practical consequences are likely to be the same, i.e., after expiration the keys will not be accepted for identification or non-repudiation.

Authentication / Verification

By providing a challenge that requires a response, it is possible to authenticate each of the two parties involved. Either may prove ownership of a certificate by responding to the challenge with an encrypted response. The response is encrypted with the end-user's or end-entity's private key. The

Sonera SmartTrust Ltd, P.O. Box 425, FIN-00051 SONERA, Elimäenkatu 17-19, Helsinki, Finland
T +358 (0) 2040 63031 F +358 (0) 2040 62730 E info@smarttrust.com www.smarttrust.com

challenging party may decrypt the response using the public key within the certificate assumed to be that of the challenged party.

The challenged party is considered authenticated if the decrypted response is verified to match the challenge. This procedure is performed from both sides, thus the server (end-entity) verifies the client authentication and the client (end-user) verifies the server.

Both sides must have - and trust - the public key corresponding to the private key used by the CA when it issued the certificates. It's imperative, therefore, that the CA is seen to be acting transparently, and that its public key is known. This is a basic requirement of a PKI, since no party would be able to implement a trusted model without there being something to trust in the first place. Put another way, it's impossible to trust a certificate unless the user is confident it was issued by a trusted CA.

<u>Example of a remote authentication process.</u>

Party 1.		**Party 2.**
I have your certificate and I trust the CA that issued it		
Please prove authenticate yourself by proving possession of the private key associated with this certificate		
I am sendig you this message: "123ABC"		I have received your message and am using my private key to encrpypt it.
I will verify your encrypted message		Here is my reply Message "'~#£$&"
I have decrypted your message with the certificate's public key. It matches that which I originally sent you. You are authenticated		

Non-repudiation / Verification

The certificate itself is a good example of a non-repudiation service. Any party, including a third party, can verify that a noted CA issued the certificate. The act of non-repudiation act is made possible through the use of a digital signature. The digital signature is created by encrypting given data with the private key specified for non-repudiation. It is to be expected that different applications would require different keys, as mentioned earlier. The data itself may be plain text, or squeezed into a tiny data format through the use of a special algorithm. The latter is often called a hash or a message digest.

The verifying party would basically apply the same technique as used when verifying at the time of authentication, i.e. by using the certified public key to match the expected values. This procedure would ensure non-repudiation at the time of action, since the receiving party should be able to check for certificate validity and revocation status. In order to provide for long term non-repudiation, a commonly accepted time-stamping service is necessary, and the timestamp should comprise part of the signed data, allowing it to be checked at a later stage. This could be done by a notary system.

Non-repudiation services have immense potential within electronic commerce, ranging from plain mail signatures to signing crucial agreements or business transactions. Remember that your real-life signature may be copied, but a thoroughly protected private key ensures that your digital signature is impossible to copy.

Smart card based key storage – the key to security

Since PKI is based on key pairs and an algorithm that creates a link between the two keys, there is one fundamental issue that must be solved.

How can I protect my private key from disclosure or misuse?
The following section will discuss and describe what we believe to be the best solution to this question.

Protecting your key information

Security issues around network- (Internet) connected personal computers are heavily debated today. One of the most discussed issues is whether it's possible for an unauthorized person to gain access to stored data, or read and alter information that has been produced prior to being sent across the network.

Sonera SmartTrust Ltd, P.O. Box 425, FIN-00051 SONERA, Elimäenkatu 17-19, Helsinki, Finland
T +358 (0) 2040 63031 F +358 (0) 2040 62730 E info@smarttrust.com www.smarttrust.com

Obviously it's difficult to protect against intruders without establishing a fault-proof firewall, but from a home-user perspective a firewall may not be wanted. Working through a firewall over which the user does not have personal control could limit the way in which the network can be used. Although you might have a bulletproof firewall at home, this is unlikely to be the only place from which you will conduct e-business in the future.

Where is it safe to store the keys used for identification, and to sign valuable agreements, documents, and orders over the Internet? The answer is within a smart card.

The most secure smart card is the PKI card

Public key infrastructure (PKI) systems build on the uniqueness and protection offered by the users' private RSA keys. The private keys should never be exposed to anyone – not even to the user. By utilizing the power of the PKI card (a smart card with a cryptoprocessor that supports RSA) the keys may be accessed and used only within the card. Once stored in the PKI card the key value will never leave the card.

It is the operating system that prevents the keys from being exposed outside the card. They can thus never be read, removed or tampered with (even by the user). User access to the card functions is via a PIN code that the user may change at any time. PKI cards are easy to use, highly portable and can be integrated with a wide range of applications. Examples of suitable applications include financial on-line services such as home banking, secure mail, and secure web services or virtual private networks (VPNs).

Remember that all smart cards are not alike - they come in many different varieties. Many cards are unable to provide support for the RSA algorithm within the card processor. And even if they do support RSA, they may be unable to handle this process very efficiently. Far too often solutions have been implemented in which the smart card is no more than a storage media for the keys. Only the PKI smart card can establish the level of security and processing speed that is required for operating in a large scale PKI.